

UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
MARSHALL DIVISION

SSL SERVICES, LLC,

Plaintiff,

v.

CITRIX SYSTEMS, INC., AND CITRIX  
ONLINE LLC,

Defendants.

Civil Action No. 2:08-cv-158-TJW

JURY TRIAL DEMANDED

**DEFENDANTS CITRIX SYSTEMS, INC. AND CITRIX ONLINE LLC'S RESPONSIVE  
CLAIM CONSTRUCTION BRIEF PURSUANT TO PATENT RULE 4-5 (b)**

## **TABLE OF CONTENTS**

	<b><u>Page</u></b>
I. INTRODUCTION .....	1
II. CONSTRUCTION OF THE DISPUTED TERMS .....	1
A. The Patents In Suit and Asserted Claims .....	1
B. General Principles Governing Claim Construction .....	4
C. Steps Of Method Claim 27 Of The ‘796 Patent And Claim 7 Of The ‘011 Patent Must Be Performed In Order .....	5
D. The Preambles of the Asserted Claims Are Limitations.....	7
E. Construction of the Disputed Terms .....	9
1. “client computer” (‘796, claim 27; ‘011 claims 2, 4, 7) .....	9
2. “means for transmitting data to and receiving data from an open network” (‘796, claim 27; ‘011 claims 2, 4, 7).....	10
3. “Intercepting function calls and requests for service” (‘796, claim 27; ‘011 claims 2, 4, 7) .....	10
a. “Intercepting” Means “Seizing” Something Intended to Go To Another, Not Merely “Receiving”.....	10
b. The “Interceptor” Is A Shim .....	12
4. “authentication and encryption program” and “encryption and authentication software” (‘796, claim 27; ‘011 claims 2, 4, 7).....	15
a. “Authentication” Is The Process Of Verifying The Identity of An Entity.....	17
5. “encrypt files” (‘796, claim 27; ‘011 claims 2, 4, 7) .....	17
6. “destination address” (‘796, claim 27).....	19
7. “intercepting a destination address” (‘796, claim 27).....	21
8. “causing said applications level authentication and encryption program to communicate with the server in order to enable the applications level authentication and encryption program to generate said session key” (‘796, claim 27).....	22
9. “recreate the session key” (‘796, claim 27) .....	24
10. “transmitting the encrypted files directly to the destination address” (‘796 patent, claim 27) .....	25
11. “mutually authenticate the server and client computer initiating communications with the server” (‘011, claims 2, 4) .....	27
12. “a shim” (‘796 patent claim 27 ‘011 patent, claims 2, 4 and 7) .....	28

13. “said function calls and requests for service/intercepted function calls and requests for service being limited to communications functions without reference to encryption” (‘011, claims 4, 7) ..... 29

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>CASES</b>	
<i>Baldwin Graphic Sys., Inc. v. Siebert, Inc.</i> , 512 F.3d 1338 (Fed. Cir. 2008).....	8
<i>Bd. of Regents of the Univ. of Texas Sys. v. BENQ Am. Corp.</i> , 533 F.3d 1362 (Fed. Cir. 2008).....	25
<i>Callicrate v. Wadsworth Mfg.</i> , 427 F.3d 1361 (Fed. Cir. 2005).....	23
<i>Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.</i> , 289 F.3d 801 (Fed. Cir. 2002).....	8
<i>Charles E. Hill &amp; Assoc. v. Amazon.com</i> , No. 2:02-CV-186, 2005 U.S. Dist. LEXIS 45414 (E.D. Tex. Oct. 7, 2005) (Ward, J.) .....	24
<i>Combined Sys., Inc. v. Def. Tech. Corp.</i> , 350 F.3d 1207 (Fed. Cir. 2003).....	5
<i>E-Pass Techs., Inc. v. 3Com Corp.</i> , 473 F.3d 1213 (Fed. Cir. 2007).....	5
<i>Flex-Rest, LLC v. Steelcase, Inc.</i> , 455 F.3d 1351 (Fed. Cir. 2006).....	21
<i>Honeywell Int’l, Inc. v. ITT Indus., Inc.</i> , 452 F.3d 1312 (Fed. Cir. 2006).....	14
<i>Markman v. Westview Instruments, Inc.</i> , 517 U.S. 370 (1996).....	5
<i>Markman v. Westview Instruments, Inc.</i> , 52 F.3d 967 (Fed. Cir. 1995), <i>aff’d</i> , 517 U.S. 370 (1996) .....	5
<i>Merck &amp; Co. v. Teva Pharms. USA, Inc.</i> , 395 F.3d 1364 (Fed. Cir. 2005).....	18
<i>NTP, Inc. v. Research In Motion, Ltd.</i> , 418 F.3d 1282 (Fed. Cir. 2005).....	24
<i>O.I. Corp. v. Tekmar Co.</i> , 115 F.3d 1576 (Fed. Cir. 1997).....	15, 16

*Omega Eng’g, Inc. v. Raytek Corp.*,  
334 F.3d 1314 (Fed. Cir. 2003).....29

*Phillips v. AWH Corp.*,  
415 F.3d 1303 (Fed. Cir. 2005) (en banc).....5

*PSC Computer Prods., Inc. v. Foxconn Int’l*,  
355 F.3d 1353 (Fed. Cir. 2004).....18

*Seachange Int’l, Inc. v. C-Cor Inc.*,  
413 F.3d 1361 (Fed. Cir. 2005).....7, 8

*Standard Oil Co. v. Am. Cyanamid Co.*,  
774 F.2d 448 (Fed. Cir. 1985).....30

*TriMed, Inc. v. Stryker Corp.*,  
514 F.3d 1256 (Fed. Cir. 2008).....10

*Visto Corp. v. Good Tech., Inc.*,  
No. 2:06-CV-039, 2008 U.S. Dist. LEXIS 3244 (E.D. Tex. Jan. 16, 2008).....5

**STATUTES**

35 U.S.C. § 112, ¶ 6.....10

**OTHER AUTHORITIES**

Local Rule 4-5(b).....1, 2

## **I. INTRODUCTION**

Pursuant to Patent Local Rule 4-5(b), and the December 18, 2008 Docket Control Order, Defendants Citrix Systems, Inc. and Citrix Online LLC (collectively, “Citrix”) submit this responsive claim construction brief for the claim terms and phrases to be construed in the asserted claims of U.S. Patent No. 6,061,796 (“the ‘796 patent”) and U.S. Patent No. 6,158,011 (“the ‘011 patent”). The ‘011 patent is a continuation of the ‘796 patent. Since the patent specifications are identical, unless otherwise noted all patent citations are to the ‘796 patent, attached as Exhibit 1.

Citrix’s proposed constructions define the claim terms in precise, understandable language that stay true to the terms’ ordinary meaning as reflected in the patents themselves. SSL’s proposed constructions, on the other hand, use deliberately imprecise and incorrect terminology wholly at odds with the claims, the specification and the prosecution history.

A few examples of SSL’s proposals highlight this: SSL asks the Court to hold that a “client *computer*” can be a person. This litigation-driven definition is squarely contradicted by what the specification teaches, what the claims require and what anyone reading the patent would understand. SSL also asks the Court to: abandon English and construe “intercepting” as “receiving”; ignore the noun “address” in “destination address”; remove “**re**” from “recreate, and interpret “directly” to include “indirectly.” In contrast, Citrix seeks constructions that are true to the ordinary meaning of the terms and that reflect the meaning of those claim elements when understood in the context of the claimed invention as a whole.

## **II. CONSTRUCTION OF THE DISPUTED TERMS**

### **A. The Patents In Suit and Asserted Claims**

Generally speaking, the ‘796 and ‘011 patents are directed to computer networks known as virtual private networks. “A virtual private network (VPN) is a system for securing

communications between computers over an open network such as the Internet.” Ex. 1 at 1:14-16.<sup>1</sup> The ‘796 and ‘011 patents claim methods and systems for securely transmitting files from one computer to the other over publicly accessible networks such as the Internet. The asserted claims are Claim 27 of the ‘796 patent and Claims 2, 4 and 7 of the ‘011 patent.

The claimed methods and systems require an authentication and encryption program as part of their security protocol. As discussed in more detail below, “authentication” is the process of verifying the identity of an entity on the network – “it is the means of gaining confidence that people [users] or things [*e.g.*, a computer] are who or what they claim to be.” Ex. 5 at 109-10. “Encryption” is the process of rendering data unintelligible without decrypting. D.I. 92 at 2. The claims require that computer files are encrypted using a “session key” before they are transmitted over the Internet. A “session key” is “a sequence of bits that is input into an encryption algorithm to encrypt data for a session.” D.I. 92 at 1. The encrypted files can be sent securely over the public Internet to another computer because the files are unintelligible until they are decrypted. In order to decrypt the files, the receiving computer must have the same session key as the sending computer.

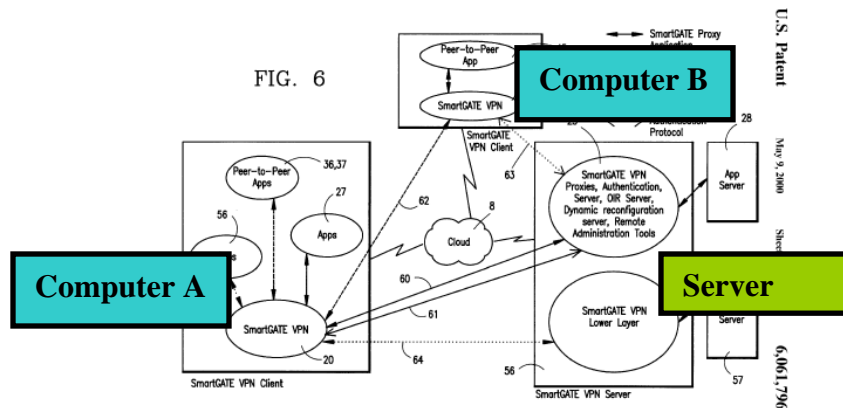
Claim 27 can be used here as exemplary claim.<sup>2</sup> It claims a method of allowing one client computer to send encrypted files *directly* to a second client computer over a “multi-tier virtual private network.” These direct communications between the two client computers are referred to throughout the patent as peer-to-peer communications. Abstract, Figs. 1A, 1B and 6, 1:27-53. The peers communicate with a server to generate and recreate the session key.

Claim 27 implements features of Figures 3-4 and 6. Figure 6 is reproduced below.

---

<sup>1</sup> “Ex. \_\_” refers to the exhibits attached to the Declaration of Andy H. Chan in Support of Citrix’s Responsive Claim Construction Brief pursuant to Patent Rule 4-5(b), filed herewith.

<sup>2</sup> The full text of claim 27 of the ‘796 patent and claim 7 of the ‘011 patent with letter labels identifying the preambles and each step of the claims are attached hereto as Exhibits 3 and 4.



As shown in the figure, the claimed VPN includes “a plurality of client computers,” and “a server,” each of which have the ability to communicate over the Internet. 27[A]. In Figure 6, client computers are labeled “Computer A” and “Computer B,” and a server is labeled “Server.” Each client computer contains “client authentication software,” “shims” (shown in Figs. 3-4), and “applications with communications capabilities,” (labeled “Peer-to-Peer App”). 10:66-11:7.

In step 27[B], an application running on Computer A attempts to open a communication link to Computer B by making “function calls and requests for service” to “a lower level set of communications drivers.” These communications drivers are software on the first client computer that allow the computer to open the communication link. *See* Figs. 2-4. Before the communications drivers can execute the function call, the function call is intercepted by a different software module on Computer A. 27[B]. The software that intercepts the function call is a “shim.” *See, e.g.,* 6:35-59, 6:66-7:6, 8:23-32, 9:42-49, 10:66-11:14, Figs. 2-4.

The interception of the function call causes “an applications level authentication and encryption program” in Computer A to communicate with the Server and generate a session key. 27[C] & [E];<sup>3</sup> *see, e.g., also* 9:42-52 (The shim intercepts a function call and “in response thereto” the “authentication client software initiate[s] communications with the authentication

<sup>3</sup> The drafting of the claim is flawed since it claims some of the same steps twice.

server”); 9:53-59; (“session keys generated during the initial communications with the authentication server”); 11:23-27 (“the invention provides for the function calls . . . to be intercepted and the initialization procedure routed through channel 61 to the authentication server”). In Figure 6, the session key generation occurs over communications link **60**. 11:21-23.

Since the claimed method involves direct communications between two client computers, Computer B needs to have the same session key as Computer A so that it can decrypt the encrypted files sent to it by Computer A. Accordingly, the shim on Computer A also intercepts the address of Computer B, and transmits it to the Server. 27[D] & [F]; *see also* 9:62-67 (“the principal function of shim 50 is to arrange for the destination of [sic] address of the communication to be supplied to . . . authentication server”).

After receiving the address of Computer B, the Server communicates with Computer B. 27[G]; *see also* 9:60-10:8 (“[t]he latter function provides the authentication server with the client address so that the authentication server can establish a secure and authenticated link with the peer application”). This communication link is shown as **63** in Figure 6. 11:22-36. The Server enables Computer B to “recreate the session key” that was previously generated in steps [C]/[E]. 27[H]; *see also* 11:24-37 (“In the case of a peer-to-peer application, in which the clients wish to communicate over a direct link **62** . . . . Server **23** then opens a secured channel **63** . . . and transmits information . . . which allows the client to recreate the channel **60** session key for use in decrypting communications sent over channel **62**”). The session key is used by Computer A to encrypt files, and the encrypted files are then transmitted *directly* – *i.e.*, they are not relayed by a server – to Computer B. 27[H] & [I]. The direct link between the two client computers is **62** on Figure 6. 11:24-37.

## **B. General Principles Governing Claim Construction**

Claim construction is an issue of law for the court to decide. *Markman v. Westview*

*Instruments, Inc.*, 517 U.S. 370, 391 (1996). To ascertain the meaning of claims, the court looks to three primary sources: the claims, the specification, and the prosecution history. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995), *aff'd*, 517 U.S. 370 (1996). The claims “must be read in view of the specification, of which they are a part.” *Id.* (citation omitted); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). The specification “is the single best guide to the meaning of a disputed term.” *Phillips*, 415 F.3d at 1315 (citation omitted).

**C. Steps Of Method Claim 27 Of The ‘796 Patent And Claim 7 Of The ‘011 Patent Must Be Performed In Order**

With respect to the method claims at issue, a fundamental question is whether the language of the claims require that the claimed steps be performed in a specific order. Citrix submits that they do, because the language of subsequent steps requires that preceding steps have already been performed. *E-Pass Techs., Inc. v. 3Com Corp.*, 473 F.3d 1213, 1222 (Fed. Cir. 2007); *Visto Corp. v. Good Tech., Inc.*, No. 2:06-CV-039, 2008 U.S. Dist. LEXIS 3244, at \*16-17 (E.D. Tex. Jan. 16, 2008) (Everingham, M.J.) (“Because the claimed steps explicitly require an order of operation, the court concludes that imposing an order to the steps is proper.”). SSL, in contrast, asserts that there is no order whatsoever to the claim steps. D.I. 98 at 28-30.

However, as already demonstrated in part above, claim 27 would be nonsensical and inoperative if the claimed steps were read out of order.<sup>4</sup> Clearly, many steps of claim 27 rely on prior steps to provide antecedent basis. The need for antecedent basis explicitly, grammatically, and logically requires that the claimed steps be performed in order. *Combined Sys., Inc. v. Def. Tech. Corp.*, 350 F.3d 1207, 1211-12 (Fed. Cir. 2003). For example, as shown in the table below, “intercepting a destination address” (27[D]), must precede the step of “transmitting *said*

---

<sup>4</sup> The sole exception is 27[D] – “intercepting a destination address” – which can occur before or after 27[C].

destination address to said server” 27[F]. In another example, a session key must be generated (27[C] &[E]) by the first client computer (Computer A) *before* the session key can be *recreated* by the second client computer (Computer B) in 27[H]. The table below provides reasoning for order of steps in Claim 27.

<b>Claim 27 Step</b>	<b>Must Precede</b>	<b>Reason</b>
27[B]: “intercepting function calls . . . sent by an applications program in one of said client computers to a lower level set of communications drivers”	All other steps.	Claimed interception causes authentication/encryption software to communicate with the server. <i>See</i> 27[C], [E]; 9:42-53; 11:24-29.
27[C]: “causing . . . program . . . to communicate with the server, generate a session key, and use the session key . . . to encrypt files . . . before transmittal over said open network”  27[E]: “causing . . . program to communicate with the server in order to enable . . . program to generate said session key”	27[F] “transmitting said destination address to said server”  27[H] “enabling said second of said two client computers to recreate the session key”  27[I]: “causing said authentication software to encrypt files to be sent to the destination address using the session key”  27[G], 27[J]	1. Communication with the server must occur before anything can be transmitted to it.  2. The session key must be generated before it can be “recreated” or used to “encrypt files.”  3. The term session key in 27[C]/[E] provides antecedent basis for “ <i>the</i> session key” in 27[H]/[I].  4. 27[F] precedes 27[G].  5. 27[I] precedes 27[J].
27[D]: “intercepting a destination address . . . .”	27[F]: “transmitting said destination address to said server”  27[I]: (see above)  27[J]: “transmitting the encrypted files directly to the destination address”  27[G], [H]	27[D] logically precedes these steps and “ <i>a</i> destination address” provides antecedent basis for “ <i>said/the</i> destination address” used in 27[F], [I] and [J].  27[G] and [H] logically must follow 27[F].
27[F]: transmitting said destination address to said server	27[G] causing said server to communicate with the second of said two client computers	27[F] logically precedes 27[G] because the server cannot communicate with the second client computer until the server knows the second

		client computer's address.
27[G] (see above)	27[H], [I], [J] (see above)	The server cannot enable the second client computer to recreate the session key (27[H]) until it communicates with the second client computer in 27[G].
27[I] (see above)	27[J] (see above)	The files must be encrypted before they can be transmitted as "encrypted files."

Claim 7 of the '011 patent likewise requires a specific order. The first step of claim 7 is similar to that of claim 27 and requires interception of specific types of function calls and requests for services to a lower level set of communications drivers. 7[B]. This "interception" causes an applications level authentication and encryption program in the first client computer to communicate with the server "*in response to receiving said intercepted function calls and requests for service* by generating a session key." 7[C]. The session key is then used to "encrypt file[s] . . ." *Id.* The term "in response to" in 7[C] demonstrates that 7[C] must come after 7[B].

#### **D. The Preambles of the Asserted Claims Are Limitations**

Another threshold dispute is whether terms appearing in the preambles of the asserted claims – claim 27 of the '796 patent and claims 4 and 7 of the '011 patent – are limitations. Contrary to SSL's assertion, in this case the preambles are limiting because they contain terms that provide "the only antecedent basis" for terms appearing in the body of the claim. *See Seachange Int'l, Inc. v. C-Cor Inc.*, 413 F.3d 1361, 1376 (Fed. Cir. 2005).

In *Seachange*, the preamble of the method claim at-issue read:

A method for redundantly storing data in a *distributed computer system having at least three processor systems*, each processor system comprising at least one central processing unit and at least one mass storage sub-system.

*Id.* at 1368 (emphasis added). The parties disputed whether "distributed computer system" is a

limitation of the method claim. *Id.* at 1375. The Federal Circuit held that it is because the method steps in the body of the claim repeatedly referred to “*said* processor systems.” *Id.* at 1376. The court explained that “[t]he preamble provides the only antecedent basis and thus the context essential to understand the meaning of ‘processor system’; therefore, the preamble, including the phrase ‘distributed computer system,’ limits the scope of the claimed invention.” *Id.* (emphasis added).

Here, the structure of claim 27 of the ‘796 patent (a method claim) is identical to that at issue in *Seachange*. Claim terms appearing in the preamble – *i.e.* “multi-tier virtual private network,” “server” and “plurality of client computers” provide the only antecedent basis for terms appearing in the steps of the method claim. *See* 27[A]. As in *Seachange*, the method steps that follow the preamble “repeatedly involve” “*said* client computers,” “*the* server” or “*said* server”<sup>5</sup> and “*said* virtual private network.” Thus, the preamble of claim 27 provides “the only antecedent basis” for these claim terms and the context necessary to understand the scope of the claimed invention. 413 F.3d at 1376.

Similarly, the preambles of claims 4 and 7 of the ‘011 patent provide the only antecedent basis for terms that appear in the bodies of the claims, namely “the server,” “the client computer,” “said function calls and requests for service,” “the lower level set of communications drivers,” and “said open network.” Claims 4 and 7 of the ‘011 patent thus rely on both the preamble and the claim body to define the claimed invention.

The case law relied upon by SSL (D.I. 98 at 27-28) makes this point. *See Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (“Additionally, dependence on a particular disputed preamble phrase for antecedent basis may limit claim scope

---

<sup>5</sup> In patent claims “the” is the same as “said.” *See Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342-43 (Fed. Cir. 2008) (“the subsequent use of definite articles ‘the’ or ‘said’ in a claim refer back to the same claim term”).

because it indicates a reliance on both the preamble and claim body to define the claimed invention.”). In urging that the preambles are not limiting (D.I. 98 at 27-28), SSL simply disregards this fundamental principle of claim construction.

**E. Construction of the Disputed Terms**

**1. “client computer” (‘796, claim 27; ‘011 claims 2, 4, 7)**

The term “client computer” means what it says – it is a machine, *i.e.*, a computer. A “*client* computer” is “a computer that uses the services provided by a server.” SSL does not dispute that a client computer “uses the services provided by a server.” Nor does SSL dispute that the term “client computer” includes computers. Instead, SSL disputes that the term “client computer” is *limited to* a computer – SSL asserts that it can also refer to a *user* of a computer. Not surprisingly, SSL offers no support for the remarkable proposition that the patent uses the term “client computer” to refer to a person.

SSL’s first citation – 4:61-65 – simply notes that the prior art SmartGate system uses session key generation to establish mutual authentication. It says nothing about what entities are participating in mutual authentication; it does not so much as hint that the term “computer” refers to a user of the computer. SSL’s reliance on 2:28-32, and on U.S. Patent No. 5,602,918 (“the ‘918 patent”) is likewise unavailing – nowhere is the term “computer” used to refer to a person. SSL extensively argues that the patents-in-suit and the ‘918 patent sometimes use the term “client” to refer to a “user.” D.I. 98 at 4-5. Whether or not that is true is an irrelevant consideration. The asserted claims do not claim a “client”; they claim a “client *computer*.”

The asserted claims themselves – through their explicit statements that the claimed “client computers” contain software – make clear that a “client computer” is a computer, not a person. Indeed, claim 4 of the ‘011 patent is directed solely to “[c]omputer software for installation on a client computer.” Claim 27 of the ‘796 patent and claims 2, 4, and 7 of the ‘011

patent all require “client computers each including means for transmitting data to and receiving data from an open network,” and client computers containing “applications level” software.

The specification likewise makes clear that “a client computer” is a computer. *See, e.g.*, 11:1-7 (“The principal components of the overall system are the client computers containing software of the type illustrated in FIGS 2-5...”); 1:43-44 (“applications on the client computers”); 6:40-42 (“network interface layers of a client computers communications hierarchy”). There is not a single recitation of the term “client computer” in the patents that suggests that a client computer is anything other than a machine – that is, a computer.

**2. “means for transmitting data to and receiving data from an open network” (‘796, claim 27; ‘011 claims 2, 4, 7)**

The parties’ sole dispute surrounding this claim term is whether it should be construed as a “means-plus-function” element pursuant to 35 U.S.C. § 112, ¶ 6. Citrix asserts that it should. A patentee’s use of the word “means” in a claim limitation creates a presumption that 35 U.S.C. § 112, ¶ 6 applies. *TriMed, Inc. v. Stryker Corp.*, 514 F.3d 1256, 1259 (Fed. Cir. 2008). SSL cannot rebut that presumption.

**3. “Intercepting function calls and requests for service” (‘796, claim 27; ‘011 claims 2, 4, 7)**

The term “intercepting function calls and requests for service” should be construed to mean “seizing by a shim an application program’s function calls and requests for service intended for another software module.”

**a. “Intercepting” Means “Seizing” Something Intended to Go To Another, Not Merely “Receiving”**

First, the term “intercept” has a straightforward and well-understood meaning – “[t]o interrupt the course of, esp. by seizing.” Ex. 6 at 362. A familiar example of “intercepting” comes from football – a quarterback throws the ball to a wide receiver but before the intended

receiver catches it, a defensive back from the opposing team seizes – *i.e.*, *intercepts* – it. The use of the terms “intercepting” and “intercept” in the asserted claims is consistent with this well-understood meaning – seizing something that is intended to go to another.

Second, the thing that is being “intercepted” in the claim is clearly spelled out in the claim language as being the “function calls and requests for service” sent by an applications program to a lower level set of communications drivers. 20:56-58; Ex. 2 at 13:15-17, 13:59-61, 14:49-51. The term “function call” has a well-understood meaning in computer science – it is “a call from a program that passes control to another software routine.” *See* Ex. 7 at 212 (“**function call**: A program’s request for the services of a particular function” and “**function**: The purpose of, or the action carried out by , a program or routine.”).<sup>6</sup> Similarly a “request for service” is a request made from an application program to the TDI layer software requesting that the TDI layer software perform a particular function. 10:30-36 (referencing “intercepting TDI service requests”).

The phrase “intercepting” as it applies to function calls and requests for service in the claim is aptly construed as “seizing” because the “function calls and requests for service” passed by one software module (the applications program) to an intended recipient software module (communications driver) are seized by an unintended recipient: software defined and identified in the patent as a “shim.” *See e.g.* 6:35-59, 6:66-7:6, 8:23-32, 9:42-49, 10:66-11:14, Figs. 2-4. As described in the specification, the intercepted function calls and requests for service are not executed by the intended software module. Rather, the shim intercepts the function calls and requests for service and then turns programmatic control over to another piece of software known as the “authentication client software.” Figs. 3-4, 9:42-10:11 (“diverted to the

---

<sup>6</sup> For example, in a computer program, the program may require that the numbers x and y be added. The function “ADD( )” contains the code that causes x and y to be added. Thus, the computer program makes the function call ADD (x, y), and control of program execution is passed to the software routine that performs addition.

authentication software”), 10:24-27 (“diverting certain information to the client software”). This is classic interception.

SSL abandons the teachings of the patents-in-suit and the English language to argue that “intercepting” means “receiving.” See D.I. 98 at 7. Not only is SSL’s definition completely contrary to the common understanding of the meaning of “intercept,” it is contrary to the teachings of the patents. Section 8:43-49 relied upon by SSL does not even describe an embodiment of the claimed inventions, but rather describes *prior art* architecture found in Figure 2 of the patent. The passage says only “client authentication software 20 intercepts interconnect calls”; it says nothing about *how* such interception occurs, nor does it suggest that it is referring to interception of function calls and requests for service sent from an applications program to a lower level set of communications drivers as the claimed inventions require. SSL’s citations to Fig. 7 and 11:66-12:2 likewise do not support its proposed definition. These citations only state that the “the applications level authentication program 20 illustrated in FIGS. 3-5 receives a call initiation request” *from* another program “*either directly*” or “*via shims.*” 11:66-12:3. This passage in no way equates “intercepting” with “receiving.”

**b. The “Interceptor” Is A Shim**

To be consistent with what the patentee repeatedly identified as its “invention” and described in the specification and file history as a critical feature of the invention, the Court’s construction of the claim phrase “intercepting function calls and requests for service” should also state that the “intercepting” function is performed by a shim.<sup>7</sup> The only “interceptor” of function calls and requests for services sent from an applications program to a lower level set of communications drivers described in the patents is a software module referred to as a “shim.”

---

<sup>7</sup> The term “shim” is defined in the discussion below at Section II.E.12.

Indeed, the use of a shim to intercept function calls and requests for services is repeatedly highlighted throughout the patents as the key feature of the claimed inventions. For example, the patent sets out a list of the objectives of “the invention.” 5:66-6:34. The paragraph immediately following explicitly states that the inventions require shims for interception:

*These objectives of the invention* are accomplished by providing a virtual private network . . . in which the clients are equipped with an applications level encryption and mutual authentication program *which includes at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computers communications hierarchy, and which intercepts function calls or data packets . . .* (6:35-43) (emphasis added).

The patent states that the invention itself is the use of shims:

In addition, it [sic] noted that the client computer architectures illustrated in FIGS. 3-6, which are modified versions of the architecture of FIG. 2, is to be used with an overall network layout such as the one illustrated in FIG 6 . . . ***The invention is not merely the addition of shims to the client software, but involves the manner in which the shims are used in the establishment of the authentications and key generation links to the server.***

8:23-32 (emphasis added); *see also* Abstract (“A virtual private network . . . uses . . . at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computer to intercept function calls, requests for service, or data packets”); 2:10-16 (“*[T]he invention* maintains the applications level infrastructure of prior client server private networking arrangements, while *adding shims to lower levels* in order to accommodate a variety of peer-to-peer communications applications . . .”) (emphasis added).

Moreover, the only “interceptor” of function calls and requests for services sent from an applications program to a lower level set of communications drivers described in the patents is a software module referred to as a “shim.” *See* Figs. 3-5 (showing socket and TDI shims); *see also* 9:42-49 (“[F]IG. 3 modifies the arrangement of FIG. 2 by adding a socket shim 50 . . . The shim 50 operates by hooking or intercepting call initiation function calls 40 made to the socket . . .”); 10:22-32 (“FIG. 4 shows the variation of the client authentication software 20 in which a TDI

shim 52 similar in function to the socket shim 50 is provided above the TDI layer . . . As with the socket shim, *TDI shims are not new and can be implemented in known manner, by intercepting TDI service requests . . .*)” (emphasis added).

Indeed, there is *no* description of intercepting function calls and requests for service from an applications program to a lower level set of communications drivers other than by using shims. In view of these facts, the scope of the inventions is limited to a “shim.” *See Honeywell Int’l, Inc. v. ITT Indus., Inc.*, 452 F.3d 1312, 1318 (Fed. Cir. 2006) (holding that the written description’s references to “this invention” or “the present invention,” and disclosure of only one embodiment limited the scope of the claims). “The public is entitled to take the patentee[s] at [their] word and the word was that the invention is a [shim].” *Id.*

The ‘011 prosecution history confirms that the claimed “interceptor” is a shim. In response to a rejection of all of the claims, including application claim 31 (which issued as claim 7 of the ‘011 patent), the patentee distinguished the claims over the prior art, stating:

In other words, instead of just providing a socket that provides encryption services as in the Elgamal patent, ***the present invention inserts a shim between the sockets layer and applications programs that use the sockets layer.*** The shim diverts function calls to an applications level encryption and authentication program in a manner that is transparent to both the socket and the applications program, and the applications level encryption and authentication program initially directs communications to an authentication server in a manner which is also transparent to the applications program and sockets layer. Ex. 10 at SSL0010157 (emphasis added).

Thus, the patentee made clear that the “interceptor” of claim 7 is a shim; the patentee so argued despite the fact that the claim does not recite a shim.

Named inventor Christopher Brook, who was represented at his deposition by SSL’s counsel, agreed. He testified in response to his own counsel’s questions that to implement the claimed inventions without a shim would require one to “invent” a new way of doing it. Ex. 9 at 196:12-197:14. Mr. Brooke also testified to his understanding of the invention as requiring

shims, stating: “A. Absolutely used shims, it's always been done that way. Why would you throw out the baby with the bathwater and start over again? *Id.* at 198:5-199:14.

Computer security expert, Dr. Angelos Keromytis, testified to having the same understanding of the claim invention. *See* Ex. 17 at 60:22-62:7, 67:24-68:2; D.I. 92-3 (Dr. Keromytis’ CV).

Although the patents describe the invention as “shims,” and describe no way of performing the claimed interception without using shims, SSL contends that claim differentiation shows that shims are not required. D.I. 98 at 9-10. SSL’s claim differentiation argument fails, however, because the claim SSL relies upon to make its argument – claim 28 – is not differentiated in its use of the word “shim.” Rather, claim 28 further limits the *location* of the shim. *See* Ex. 1, claim 28 (“a shim positioned between a peer-to-peer applications program and a layer”). In any event, claim differentiation cannot alter a definition that is otherwise clear from the claim language, written description, and prosecution history. *O.I. Corp. v. Tekmar Co.*, 115 F.3d 1576, 1582 (Fed. Cir. 1997). Thus, even were claim differentiation applicable, since the patents only describe using a “shim” to perform the claimed interception, and refer to “shims” as “the invention,” the scope of the claims is still limited to interception by a shim. *See, e.g., Versata Software, Inc. v. SAP Am., Inc.*, 2:07-CV-153, 2009 U.S. Dist. LEXIS 45751, at \*17-18 (E.D. Tex. May 19, 2009) (Everingham, M.J.) (disregarding plaintiff’s claim differentiation argument because the specification limited the scope of the invention).

**4. “authentication and encryption program” and “encryption and authentication software” (‘796, claim 27; ‘011 claims 2, 4, 7)**

“Authentication and encryption program” and “encryption and authentication software” mean what they say – they are “software that performs authentication and encryption.” The sole dispute concerning the meaning of this term arises from SSL’s desire to rewrite the claim term to

read “authentication *or* encryption software.” Paradoxically, while dismissing the claim element “authentication and encryption program/software” as a “label,” SSL advises that “it is only the claims themselves that set forth the intended scope.” D.I. 98 at 11. Of course, this ignores that the “authentication and encryption program” *is* an element of each of the claims, and thus imposes a limitation on claim scope that SSL cannot simply read out of the claims.

SSL irrelevantly notes that throughout the specification various terms are used to describe authentication software, and from this concludes that this evidences an “intent” to “have the specification describe the exemplary functions” of the claimed authentication and encryption program/software. D.I. 98 at 12 (emphasis omitted). The flaw in SSL’s reasoning is that *nowhere* does the specification describe an “authentication and encryption program” as performing authentication *or* encryption but not both. And, as SSL concedes, the specification describes programs that provide both authentication and encryption. *See, e.g.*, 11:65-12:19.

Equally flawed is SSL’s argument that the claimed program/software need not perform authentication and encryption because the specification does not state that such a program is an *essential* component of the inventions. D.I. 98 at 12. Whether such a program is *essential* is irrelevant – the patentees *claimed* an authentication and encryption program.

SSL’s prosecution history argument (*id.*) likewise fails, because it misrepresents the record. The claim that was filed as claim 33 (and issued as claim 27), originally depended from claim 31, and cryptically claimed an “authentication and encryption program” that “carr[ied] out functions a.) and b.)” Ex. 8 at SSL0000076. The examiner rejected claim 33 as indefinite because there was “insufficient antecedent basis” for the term “functions a.) and b.).” *Id.* at SSL0000105. The patentees re-wrote claim 33 to be independent and eliminated the indefinite term “functions a.) and b.).” *Id.* at SSL0000358. This does not, as SSL says, evidence removal

of a “mutual authentication function” from the claim.

**a. “Authentication” Is The Process Of Verifying The Identity of An Entity**

Although SSL previously stated that it disagreed with Citrix regarding the meaning of “authentication,” and “authenticate” (*see* D.I. 92-1 at 10), it nowhere provides a definition for those terms.<sup>8</sup> As discussed above, “[a]uthentication” is the process of verifying the identity of an entity on a network – “it is a means for gaining confidence that people [users] or things [*e.g.*, a computer] are who or what they claim to be.” Ex. 5 at 109-10 (“Authentication gives *assurance of identity*. . . . Principals of various physical forms may need to be authenticated, for example, people, pieces of equipment, or running applications in computer systems.”). The ‘918 patent incorporated by reference –2:27-32 – confirms that “authentication” is “verification of *identity*.” Ex. 11 at 3:21-27 (“a method of establishing the identity”), 4:32-42 (“establish to their mutual satisfaction the identity of both the gateway processor and the client”), Figs. 3A & 3B.

SSL apparently no longer disputes the correctness of Citrix’s definition since it did not provide a definition of “authentication” or “authenticate” in its briefing to the Court. However, to the extent there is still a dispute, SSL’s prior definition was deficient because it does not explain what is being verified or validated – *i.e.*, *identity*.

**5. “encrypt files” (‘796, claim 27; ‘011 claims 2, 4, 7)**

The parties agree that “encrypt” means “to render unintelligible without decrypting.” D.I. 92 at 2. The parties dispute the meaning of the term “files.” Citrix contends that the term “files” should be given its ordinary meaning in computer science: “A collection of related data or program records treated as a basic unit of storage.” *See* Ex. 7 at 194. SSL asserts that the patentee acted as his own lexicographer and gave a special meaning to the term “files.” D.I. 98

---

<sup>8</sup> In its brief, SSL states that it proposed a construction for “authentication” at page 11. *See* D.I. 98 at 21. SSL’s brief, however does not contain a proposed definition for “authentication.”

at 12-13. But when a patentee acts as his own lexicographer, the patentee must clearly express that intent in the written description. *Merck & Co. v. Teva Pharms. USA, Inc.*, 395 F.3d 1364, 1370 (Fed. Cir. 2005). That did not occur here.

SSL asserts that the patentee defined “files” to mean any “collection or segment of data” D.I. 98 at 12, and that the term “files” thus includes “datagrams” and “packets.” *Id.* at 14. The patents, however, expressly distinguish between “files” and “packets” and “datagrams,” and make clear that they are not the same thing. The patents state that datagrams or packets *carry* encrypted files. 8:61-67 (“[I]t is to be understood that *datagrams or packets* 31 *carry* both the communications used to establish the secure channel, and the *encrypted files* subsequently sent therethrough.”) (emphasis added).

Moreover the same section plainly distinguishes between “communications used to establish the secure channel” and “encrypted files” that are subsequently sent over the secure channel. *Id.*, *see also* 9:47-58 & Fig. 3 (“The shim 50 operates by hooking or intercepting call initiation function calls 40 made to the socket . . . . Shim 50 also causes files 41 intended for the TDI layer to be diverted to the authentication software for encryption . . . and transmission as encrypted files”), 10:59-65 (noting that “IP packets are not distinguishable by content” and the “network driver layer shim” could be used to further encrypt already encrypted files), Fig. 6 & 11:49-57 (encryption of packets and datagrams). Although the specification discusses encrypting packets and other data, the claims define the scope of the patent protection and here, the patentee claimed encrypting “*files*.” The term cannot be interpreted to include “packets,” “datagrams” or other types of communications. *PSC Computer Prods., Inc. v. Foxconn Int’l*, 355 F.3d 1353, 1360 (Fed. Cir. 2004) (holding that unclaimed alternative matter disclosed in the specification is dedicated to the public).

The patent is not to the contrary. The section of the specification relied upon by SSL to argue that “files” and communications are synonymous is a reference to the prior art (*see* 8:33-34 and Fig. 2 (labeled “prior art”)), and states only that “*data communications*” from an *application* are encrypted and are “encrypted files” before they ever exit the application layer. *See* 8:56-61 & Fig. 2 (showing encrypted files 35 at the application layer). This passage does nothing to expand the meaning of “files” beyond its ordinary meaning in computer science. First, a transmission of an “encrypted file” is one type of “communication” that can occur between computers. Second, the described “encrypted files” are at the application layer; this passage cannot be a reference to encryption of “datagrams” or “packets.” As the patent makes clear, it is *the TDI layer* (below the application layer) where datagrams or packets are formed. 8:50-52 (“causing the TDI layer to form datagrams or packets”), Figs. 2-5. “Encrypted files” from the application layer cannot be a datagram or packet.

SSL’s reliance on 11:65-12:19 and Figure 7 is likewise unavailing. “Encrypted files” are a subset of “encrypted communications.” There is no indication that the term “communications” is used synonymously with “files” as SSL asserts, and the *claimed* inventions are limited to encryption of “files.” The claim language recited by SSL in support of its construction (D.I. 98 at 13), actually undermines it. It distinguishes between “files” and “packets,” and demonstrates that when patentees intended to claim encryption of packets they knew how to do so.

Finally, SSL’s argument that Citrix’s definition of “files” must be wrong because it is not featured prominently in the specification likewise fails. Since Citrix contends that “files” is to be given its ordinary meaning, there is no need to highlight the term in the specification.

#### **6. “destination address” (‘796, claim 27)**

Citrix submits that the term “destination address” means “the network layer identifier of the location on the network of the second client computer, which for Internet communications is

the IP address of the second client computer.” This construction is supported by the specification and the plain meaning of “address” as used in computer networks.

The patents make plain that “address” means “address.” The term “destination *address*” is used in the patents to refer to an *address* field found in an IP header when using an IP-based protocol to send data over the Internet:

In the case of *Internet communications*, the most commonly used set of software routines for the transport or TDI layer, which takes care of the data formatting and addressing, is the TCP/IP protocol, in which . . . *the internet protocol (IP) further packages the TCP datagrams into packets by adding additional headers used in routing the packets to a destination address.*

3:16-24 (emphasis added); *see also* 10:43-47 (“At [the NDIS] layer, *the shim 55 intercepts IP packets* from applications 56, but instead of referring back to the applications level routine, checks the *destination address* (which can be in TCP format, UDP format, and so forth) . . .”); 9:42-10:11 (“destination address” is “client address”).

The intrinsic evidence – art cited during prosecution of the ‘796 patent (Hedrick) – confirms that the “destination address” of an IP packet refers to an actual address – *i.e.*, the “IP-address” of the destination computer. Ex. 8 at SSL0000385-410. Hedrick explains that when the TCP/IP protocol is used to effectuate communications between two computers over the Internet, the IP protocol adds a “header” to TCP datagrams that has a field called “source address” and “destination address.” *Id.* at SSL0000392. It explains that “source address” and “destination address” are both “32-bit addresses, like 128.6.4.194,” and that the “source address” is “simply the address of your machine” while the “destination address” is “the address of the other machine.” *Id.* Hedrick also explains that the “destination address” mechanism is the same for other IP-based protocols such as UDP and ICMP. *Id.* at SSL0000399.

The plain meaning of the term “address” at the time the patent application was filed is wholly consistent with the intrinsic evidence and Citrix’s proposed construction. *See* Ex. 12. at

16 (“**address:3.** In the *Internet*, the location of a host on the network. *See IP address*”); *id.* at 270 (“**IP-address:** A 32-bit *binary number* that uniquely and precisely identifies the location of a particular computer on the *Internet*”); *see also* Ex. 13 at 1:16-19 (“The network layer identifies the source and destination devices by their network addresses, such as an IP address.”). A person of skill would also understand the term “destination address” to have the meaning advanced by Citrix. *See* Ex. 17 at 56:24-57:3, 98:4-99:2.

In defining the term “destination address,” SSL improperly writes the term “address” out of the claim, and instead provides a construction for “destination.” D.I. 98 at 15. However, it is “basic patent law doctrine that every limitation of a claim is material.” *Flex-Rest, LLC v. Steelcase, Inc.*, 455 F.3d 1351, 1361 (Fed. Cir. 2006). SSL attempts to justify its disregard for the claim term “address” by arguing that the terms “destination,” and “destination address” are used interchangeably. D.I. 98 at 15. SSL proffers *no* explanation for this contention.

Finally, contrary to SSL’s argument, the context of claim 27 itself makes clear that the term “destination address” as used in the claim refers specifically to the address on the network of the claimed second client computer. Claim 27 claims a method for allowing a first client computer to send encrypted files directly to a second client computer over a network. One step in the process, is “intercepting a *destination address* during initialization of communications between said one of said client computers and *a second of said client computers* on said virtual private network.” 27[D]. Moreover, the “destination address” is transmitted to the server so that the server can open a communication link with the second client computer. 27[F], [G]. “Encrypted files” are transmitted directly from the first client computer to the “destination address.” 27[J]. The “destination address” is necessarily that of the second client computer.

#### **7. “intercepting a destination address” (‘796, claim 27)**

The term “intercepting a destination address” means “seizing by a shim a destination

address.” Citrix’s proposed definition is supported by the intrinsic evidence. SSL’s proposed definition is flawed for the same reasons previously discussed regarding “intercepting function calls and requests for service” and “destination address.” *See* Sections II.E. 3 and 6, *supra*.

Again, the invention as described in the patent requires the use of a shim, and the *sole* description of “intercepting a destination address” involves interception by a shim. Indeed, for direct communications between two client computers the patent teaches:

[T]he *principal function of shim 50* is to arrange for the destination address of the communication to be supplied to both the authentication client software and to authentication server . . . .

*See* 9:42-10:11 (emphasis added). Accordingly, interception by a shim is required.

**8. “causing said applications level authentication and encryption program to communicate with the server in order to enable the applications level authentication and encryption program to generate said session key” (‘796, claim 27)**

With respect to this limitation, the parties’ dispute is focused on what is meant by causing the authentication and encryption program to communicate with the server “*in order to enable* the authentication and encryption program to generate said session key.” The plain language of claim 27 itself requires that the session key is generated *through communications* between the program running on the client computer and the server. The term means “the applications level authentication and encryption program in the first client computer produces the session key through communications with the server.”

The term “enable” means that the program’s communication with the server is essential to the generation of the session key, and that the session key is generated during communication with the server. Moreover, in a subsequent step, the server “enables” the second client computer to “recreate the session key.” 27[H]. As discussed below, the session key must be created, through communications with the server before it can be recreated.

As discussed in Section II.A above, the specification also supports Citrix's definition. The generation of the session key is described with reference to Figure 6. The interception of "function calls and requests for service" causes "an applications level authentication and encryption program" in the first client computer to communicate with the server and generate a session key. *See e.g.*, 9:42-59 (communication with server occurs "in response" to interception of function call and the "session keys [are] generated during the initial communications with the authentication server"), 11:23-29 (initialization procedure routed through server). In Figure 6, the communications link that allows for this generation of the session key is shown as **60**. *Id.* at 11:16-22 ("with arrow **60** representing the client/server response channel used to authenticate the parties and generate the session key").<sup>9</sup> The specification also explains that the second client computer "*recreate[s] the channel 60 session key* for use in decrypting communications sent over channel 62," a "direct link" between the two computers. *Id.* at 11:29-40.

Thus, the plain language of claim 27 – *i.e.*, "in order to enable," the subsequent steps of claim 27, and the patent specification make clear that the session key is generated through communication between the application level authentication and encryption program on the first client computer and the server.

SSL's construction is wrong because it disregards the phrase "in order to enable." SSL asks the Court to construe the claim to require merely that the authentication and encryption program (1) "communicate with the server" and (2) subsequently "generate said session key" in an unspecified manner that may or may not be related to the communication with the server. Thus, SSL improperly reads the phrase "in order to enable" out of the claim entirely. *Callicrate v. Wadsworth Mfg.*, 427 F.3d 1361, 1369 (Fed. Cir. 2005) (rejecting the district court's claim

---

<sup>9</sup> The specification also explains that: "For the lower level application 56 . . . the communications link to the authentication server is used to generate a session key . . ." 11:50-54 & Fig. 6.

construction as “overbroad” because it read the term “preformed” out of the claim).

#### 9. “recreate the session key” (‘796, claim 27)

The term “recreate the session key” means “reproduce the same session key previously created.” Citrix’s construction is supported by the plain meaning of the verb “recreate” – to produce something that was produced before *again*. SSL argues that this term does not require *re*-creation and asserts (without support) that the term “recreate” is synonymous with “generate.”

Citrix’s construction flows from the context of the claim itself. The disputed claim term reads “recreate *the* session key.” The use of the definite article “the” here requires that “session key” have an antecedent basis, which is necessarily a session key referenced earlier in the claim steps. *See, e.g., NTP, Inc. v. Research In Motion, Ltd.*, 418 F.3d 1282, 1306 (Fed. Cir. 2005) (construing claim term employing the definite article “the” as requiring antecedent basis); *see also Charles E. Hill & Assoc. v. Amazon.com*, No. 2:02-CV-186, 2005 U.S. Dist. LEXIS 45414, at \*45-46 (E.D. Tex. Oct. 7, 2005) (Ward, J.). The antecedent basis for “recreate the session key” is the reference to the earlier generation of the session key in 27[C] (“causing an applications level authentication and encryption program . . . to communicate with the server, generate *a session key*, and use the session key . . .”), and 27[E]. Thus, the claim term here refers back to the *same* session key that was generated in the earlier claim terms.

Citrix’s construction is also consistent with the ‘796 patent’s specification and the illustration of how the alleged invention is implemented in Figure 6. *See*, discussion of Figure 6, *supra*, at 5-6, 20. The specification explains how two client computers that want to exchange encrypted files directly come into possession of the same session key. The first client computer generates the session key in the course of communication with a server. 11:15-22; Fig. 6 (item 60). The server either (1) sends the session key to the second client computer or (2) sends information to the second client computer that allows the second client computer to recreate the

session key. *Id.* at 11:23-40 (the server “transmits information . . . which allows the client to recreate the channel 60 session key”), Fig. 6 (items 62 and 63), *see also* 9:60-10:11 (“transmit the session key to the peer application or *at least enable the peer application to recreate the session* so that it can decrypt the encrypted files received directly from the client application.”) (emphasis added). In claim 27, the patentees chose to claim an embodiment in which the previously existing session key is recreated.

SSL’s proposed construction not only ignores the language of the claim and the teachings of the specification, it runs afoul of plain English. SSL’s construction takes the “re” out of “recreate.” One cannot “recreate” a session key – if that key does not already exist. SSL’s argument that the term “recreate” is “interchangeable” with “generate” is unsupported, and ignores the fact that the patentees used the term “generate” with reference to the session key three separate times in claim 27 *before* the “recreation” step. The choice to use the different word “recreate,” creates a presumption that the patentees intended a different meaning for that word. *See Bd. of Regents of the Univ. of Texas Sys. v. BENQ Am. Corp.*, 533 F.3d 1362, 1371 (Fed. Cir. 2008) (“Different claim terms are presumed to have different meanings.”) SSL cannot rebut that presumption here.

**10. “transmitting the encrypted files directly to the destination address”  
('796 patent, claim 27)**

The parties’ dispute centers on what “*directly*” means. Citrix contends that this term means “transmitting the encrypted files to the destination address without being relayed by a server.” Citrix’s proposed construction comports with the plain language of the claim and the teachings of the specification. SSL’s definition is wrong because it requires that the Court construe “directly” to mean “indirectly.”

The patent discloses two ways in which two client computers can communicate over a

virtual private network: (1) through a server (Fig. 1A); or (2) directly (Fig. 1B); *see also* 1:26-53. Indeed, the patent repeatedly distinguishes between communications through a server, and direct peer-to-peer communications. *See, e.g.*, Abstract. 9:42-10:11, 11:16-49. Moreover, the patent refers to communications between two client computers that rely upon a server as “indirect.” 7:11-12 (“indirect authentication of peer applications by the now trusted server”).

Claim 27 explicitly requires direct transmission of encrypted files from the first client computer to the second client computer. The plain language thus precludes communications between the two client computers over a VPN occurring through a server, as shown in Figure 1A. As discussed in II.E.6 above, the “destination address” to which encrypted files are transmitted “directly,” is the address of the second client computer on the network. Thus, a packet carrying encrypted files over the Internet would have the address of the second client computer in its “destination address” field. This precludes a scenario in which transmission of the encrypted files are relayed by a server.

If transmission of encrypted files from the first client computer were “relayed by a server,” the “destination address” would be the address of the server *not* the address of the second client computer. After receiving the transmission, the server would be required to change the destination address to the address of the second client computer. That is not what is meant by transmitting *directly*.

The specification confirms that Citrix’s definition is correct. The use of a server “to establish a session key which can be used for *further direct communications* between the parties” is described throughout the patent. *See, e.g.*, 4:17-27, 9:60-10:11, 11:22-36. This direct link is shown as **62** in Figure 6, and explicitly excludes a configuration in which encrypted files are transmitted to a server, and then relayed by the server to the second client computer.

Other intrinsic evidence – prior art cited during prosecution of the ‘796 patent – also confirms that direct transmission precludes the “relaying by a server” scenario described above. *See* Ex. 8 at SSL0000292-298 at 4:3-26, 5:12-23, 7:24-8:19 (distinguishing between “direct” communications between two computers, and communications in which a communication from a first computer is transmitted to an intermediary computer (motherboard), readdressed and then transmitted to a second computer).

The extrinsic evidence is consistent. *See* Ex. 14 at 2:3-5, 2:25-29, 5:8-17, 7:20-24 (distinguishing between “direct connections,” and those that make use of Intermediate servers”); Ex. 15 at 24:1-7 (using the term “direct” to “describe a data transfer [where] no data passes through the central server”); Ex. 16 at 2 (explaining the difference between a “direct peer-to-peer connection” and “relaying through our server”).

In framing the dispute, SSL feigns ignorance as to what Citrix means when it uses the phrase “not relayed by a server” to define “directly.” SSL engages in an off-point discussion of “the cloud,” discussing “intermediate relay points (e.g., servers, routers, etc.)” and providing unsupported assertions about the necessity of servers to relay communications over the Internet. D.I. 98 at 20-21. Although SSL claims that “directly” should have its plain and ordinary meaning, SSL clearly intends to construe it to mean “indirectly,” such as when communications between two client computers are effectuated through a server as shown in Figure 1A. Such an interpretation, however, improperly reads the term “directly” out of the claim.

**11. “mutually authenticate the server and client computer initiating communications with the server” (‘011, claims 2, 4)**

As previously explained, the term “authenticate” means “to verify the identity of an entity.” *See* Section II.E.4, *supra*. “Mutual” authentication is where two entities communicating on a network verify one another’s identity. Ex. 5 at 130 (“Mutual authentication,

in which both parties to a communication session need to authenticate each other, is frequently an important requirement”). Thus, the claim term means “the server verifies the identity of the client computer and the client computer verifies the identity of the server.”

The ‘918 patent, which is incorporated by reference (2:27-32), also confirms that “mutual authentication” is a process in which two entities to a communication verify one another’s identity. Ex. 11 at 4:32-42 & 5:1-29. In this case, the claims explicitly recite the two entities to be authenticated – the “client computer” and “the server.”

## 12. “a shim” (‘796 patent claim 27 ‘011 patent, claims 2, 4 and 7)

The term “shim” should be defined as “ software that is added between two existing layers and which utilizes the same function calls so that the existing layers do not need to be modified.” The term “shim” is expressly defined in the patent:

If possible, it is generally desirable to minimize modification of the existing levels by adding *a layer to perform the desired functions, calling upon the services of the layer below, while utilizing the same function calls so that the higher layer also does not need to be modified. Such a layer is commonly referred to as a “shim.”* 3:60-66 (emphasis added).

Thus, the patent discloses that a shim is software added between two existing layers (“the higher layer” and “the layer below”), and which utilizes the same function calls so that the existing layers do not need to be modified. *See also* Figs. 3-5 (depicting shims).

The prosecution history further informs the meaning of the term “shim.” During prosecution of the ‘011 patent, the patentee defined “shim” in order to distinguish the claimed inventions from the prior art:

[I]nstead of just providing a socket that provides encryption services as in the Elgamel patent, *the present invention inserts a shim between the sockets layer and applications programs* that use the sockets layer. The shim diverts function calls to an applications level encryption and authentication program.... There is *no need to modify either the sockets layer or the applications program* by adding new function calls as taught by Elgamel... Ex. 10 at SSL0010157 (emphasis added).

SSL contends that “shim” does not need to be construed and should be given its plain and ordinary meaning, and admits that the specification discloses and teaches what “shims” are and how they are used. D.I. 98 at 22. But, SSL also argues that the way “shims” are used in the claimed invention is not disclosed in the specification, and asks the Court to ignore the express teachings of the specification. D.I. 98 at 23-24. The patent expressly describes what a shim is in the intrinsic evidence; SSL proffers no reason for deviating from this explicit definition.

In addition, a person of skill would have the same understanding the meaning of the term “shim.” *See* Ex. 17 at 68:11-69:13.

The patent also teaches what a “shim” is not. The patent discusses SmartGATE™ client software and states:

[A]lthough this program is placed between the Winsock layer and the applications, *it does not function as a shim, however, because it only affects communications directed to the authentication server.* 5:8-11 (emphasis added).

Thus, the patentees defined the scope of the term “shim” within the context of the claimed inventions. Because the patentee unequivocally disavowed a certain meaning by explaining what a shim is not, “shim” should be construed congruent with the scope of the disavowal. *See Omega Eng’g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1324-25 (Fed. Cir. 2003).

**13. “said function calls and requests for service/intercepted function calls and requests for service being limited to communications functions without reference to encryption” (‘011, claims 4, 7)**

The claimed element has two parts: (1) “said function calls and requests for service” and (2) “being limited to communications functions without reference to encryption.” The dispute between the parties centers on the meaning of “being limited to communications functions without reference to encryption.” The term means “ordinary, unmodified function calls and requests for service having no reference to encryption functions.”

The ‘011 prosecution history confirms this is the correct definition – the patentee defined

the phrase during prosecution. The patentee amended the claims by adding the phrase to overcome a prior art rejection. *See* Ex. 10 at SSL0010168-71. The patentee stated:

The claimed invention can be used in connection with **any** set of already installed communications drivers, and with any applications program capable of using the communications drivers, by simply installing a shim that intercepts calls to the communications drivers, *without the need to modify the applications program to issue a modified set of function calls in order to invoke the encryption and authentication functions. By intercepting ordinary function calls, without reference to encryption functions*, the claimed invention can be used with **any** application and any set of communications drivers. *In contrast, an application program that uses the secure sockets layer for encryption is required to use a special, modified set of function calls* in order to request encryption, thus limiting the encryption function to applications written specifically for the secure sockets layer. Ex. 10 at SSL0010171 (emphasis added).

The patentee argued that the foregoing distinguished the claimed invention over the prior art, (*id.*), and the examiner subsequently allowed the amended claims.

Despite the patentee's representations to the Patent Office, SSL maintains that the "patentee's statement was not limiting claim scope." D.I. 98 at 27. But the prosecution history limits the interpretation of claims so as to exclude any interpretation that has been disavowed during prosecution to obtain claim allowance. *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 452 (Fed. Cir. 1985). SSL's proposed definition violates this long-standing principle by inserting "explicitly reference" and "encryption protocol (e.g., secure sockets layer (SSL))" into the definition of "without reference to encryption." Indeed, SSL's proposed definition is contrary to the prosecution history and lacks evidentiary support.

Accordingly, the Court should construe the claim term to mean "ordinary, unmodified function calls and requests for service having no reference to encryption functions."

Dated: April 22, 2011

Respectfully submitted,

/s/ Erica D. Wilson

Erica D. Wilson

[ewilson@goodwinprocter.com](mailto:ewilson@goodwinprocter.com)

California State Bar No. 161386  
Thomas F. Fitzpatrick  
California State Bar No. 193565  
[tfitzpatrick@goodwinprocter.com](mailto:tfitzpatrick@goodwinprocter.com)  
Andy H. Chan  
California State Bar No. 242660  
[achan@goodwinprocter.com](mailto:achan@goodwinprocter.com)  
GOODWIN PROCTER LLP  
135 Commonwealth Drive  
Menlo Park, CA 94025  
(650) 752-3100 (Telephone)  
(650) 853-1038 (Facsimile)

J. Anthony Downs  
Massachusetts State Bar No. 552839  
[jdowns@goodwinprocter.com](mailto:jdowns@goodwinprocter.com)  
Lana S. Shiferman  
Massachusetts State Bar No. 645024  
[lschiferman@goodwinprocter.com](mailto:lschiferman@goodwinprocter.com)  
GOODWIN PROCTER LLP  
53 State Street  
Boston, MA 02109  
(617) 570-1000 (Telephone)  
(617) 523-1231 (Facsimile)

Jennifer Parker Ainsworth  
Texas State Bar Number 00784720  
[jainsworth@wilsonlawfirm.com](mailto:jainsworth@wilsonlawfirm.com)  
WILSON, ROBERTSON  
& CORNELIUS, P.C.  
900 ESE Loop 323, Suite 400  
P. O. Box 7339 [75711]  
Tyler, Texas 75701  
(903) 509-5000 (Telephone)  
(903) 509-5092 (Facsimile)

Counsel for Defendants  
Citrix Systems, Inc. and Citrix Online

**CERTIFICATE OF SERVICE**

This is to certify that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3) on this 22nd day of April, 2011. Any other counsel of record will be served by first class mail.

/s/ Erica D. Wilson

Erica D. Wilson